CLAIMS

WHAT IS CLAIMED IS:

~~1. A machine-executable method for executing a trusted command issued by a user, said method comprising the steps of:~~

~~(a) parsing the trusted command in an untrusted computing environment to generate a parsed command;~~

~~(b) submitting the parsed command to a trusted computing environment; and~~

~~(c) executing the parsed command in the trusted computing environment.~~

~~2. A method including the steps of claim 1 and additionally including the steps, executed after step (b) of claim 1, of:~~

~~(1) in the trusted environment, displaying a representation of the parsed command to the user;~~

~~(2) receiving a signal from the user signifying whether the displayed representation accurately represents the user's intentions;~~

~~(3) if the signal signifies that the displayed representation does not accurately represent the user's intentions, then preventing the performance of step (c) of claim 1.~~

~~3. The method of claim 2 wherein the representation of the parsed command is displayed, and the signal from the user is received, through a trusted path.~~

~~4. The method of claim 1 wherein the trusted computing environment comprises a security kernel.~~

~~5. The method of claim 1 wherein the untrusted computing environment comprises a general operating system.~~

~~6. A method for executing in a computing system a trusted command issued by a user, said method comprising the steps of:~~

~~(a) receiving user identification data from the user via a trusted path;~~

~~(b) receiving the trusted command from the user via an untrusted path;~~

~~(c) parsing the trusted command in an untrusted computing environment to generate a parsed command;~~

~~(d) submitting the parsed command to a trusted computing environment;~~

~~(e) in the trusted computing environment, performing a security check on the parsed command and user identification data; and~~

~~(f) in the trusted computing environment, executing the trusted command.~~

7. The method of claim 6, wherein the security check enforces an Orange Book security criterion.

8. A method including the steps of claim 6 and additionally including the steps, executed after step (d) and before step (f) of claim 6, of:

(1) in the trusted environment, displaying a representation ~~of the~~ a parsed command to the user;

(2) receiving a signal from the user signifying whether the displayed representation accurately represents the trusted command; and

(3) if the signal signifies that the displayed representation does not accurately represent the trusted command, then preventing the performance of step (f) of claim 6.

~~9. A method including the steps of claim 6 and additionally including the steps, executed after step (d) and before step (f) of claim 6, of:~~

~~(1) in the trusted environment, displaying a representation of the parsed command to a second user;~~

~~(2) receiving a signal from the second user signifying whether the displayed representation accurately represents a legitimate command; and~~

~~(3) if the signal signifies that the displayed representation does not accurately represent a legitimate command, then preventing the performance of step (f) of claim 6.~~

~~10. A method for ensuring the existence of a trusted path in a computing system comprising the steps of:~~

(a) in a trusted computing environment, upon login by a user, assigning a process identifier to the user in the trusted computing environment;

(b) storing the assigned process identifier in trusted memory;

(c) establishing a trusted path;

(d) in the trusted path, displaying the process identifier to the user; and

(e) upon a subsequent entry into the trusted path, displaying the process identifier to the user.

11. The method of claim 10 wherein the process identifier is a randomly or pseudo-randomly generated group of alphanumeric characters.

12. The method of claim 11 wherein the process identifier is pronounceable.

~~13. An automatic data processing machine programmed to execute the method of any one of claims 1 to 12.~~

~~14. An automatic data processing machine comprising means for performing the method steps of any one of claims 1 to 12.~~

~~15. A program storage device readable by a machine and tangibly embodying a representation of a program of instructions adaptable to be executed by said machine to perform the method of any one of claims 1 to 12.~~

16. Apparatus for executing a trusted command that is issued by a user and that is parsed by untrusted parsing means to generate a parsed command, comprising:

(a) trusted means for receiving the parsed command; and

(b) trusted means for executing the parsed command.

17. Apparatus for controlling the execution by a machine of a trusted command that is issued by a user and that is parsed by untrusted parsing means to generate a parsed command, comprising:

(a) trusted-program storage means, readable by the machine, for causing the machine to receive the parsed command from the untrusted parsing means; and

(b) trusted-program storage means, readable by the machine, for causing the machine to execute the parsed command.

~~18. Apparatus for controlling the execution by a machine of a trusted command that is issued by a user with user identification data and that is parsed by untrusted parsing means to generate a parsed command, comprising:~~

~~(a) trusted program storage means, readable by the machine, for causing the machine to receive the user identification data from the user;~~

~~(b) trusted program storage means, readable by the machine, for causing the machine to receive the parsed command from the untrusted parsing means;~~

~~(c) trusted program storage means, readable by the machine, for causing the machine to perform a security check on the parsed command and a security check on the user identification data; and~~

~~(d) trusted program storage means, readable by the machine, for causing the machine to execute the trusted command.~~

~~19. Apparatus as in claim 18 and additionally comprising:~~

~~(1) trusted program storage means, readable by the machine, for causing the machine to display a representation of the parsed command to the user;~~

~~(2) trusted program storage means, readable by the machine, for causing the machine to receive a signal from the user signifying whether the displayed representation accurately represents the trusted command; and~~

~~(3) trusted program storage means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command does not accurately represent the trusted command.~~

~~20. Apparatus as in claim 18 and additionally comprising:~~

~~(1) trusted program storage means, readable by the machine, for causing the machine to display a representation of the parsed command to a second user;~~

~~(2) trusted program storage means, readable by the machine, for causing the machine to receive a signal from the second~~

~~user signifying whether the displayed representation accurately represents a legitimate command; and~~

~~(3) trusted program storage means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command does not accurately represent a legitimate command.~~

add A1